1. Record Nr. UNINA9910476756103321

Titolo	Security risk management for the Internet of Things : technologies and techniques for IoT security, privacy and data protection / / edited by John Soldatos
Pubbl/distr/stampa	Norwell, Massachusetts : , : Now Publishers, , [2020] ©2020
Descrizione fisica	1 online resource (288 pages)
Disciplina	004.678
Soggetti	Internet of things
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Frontmatter / John Soldatos -- 1. Introduction / John Soldatos -- 2. Security Data Modelling for Configurable Risk Assessment as a Service in IoT Systems / Nikos Kefalakis, Angela-Maria Despotopoulou, Spyridon Evangelatos, John Soldatos -- 3. Data-driven IoT Security Using Deep Learning Techniques / Astaras Stefanos, Nikos Kefalakis, Angela-Maria Despotopoulou, John Soldatos -- 4. Privacy Awareness, Risk Assessment, and Control Measures in IoT Platforms: BRAIN-IoT Approach / Mohammad Rifat Ahmmad Rashid, Davide Conzon, Xu Tao, Enrico Ferrera -- 5. IoT Network Risk Assessment and Mitigation: The SerIoT Approach / Gianmarco Baldini, Piotr Frohlich, Erol Gelenbe, Jose Luis Hernandez-Ramos, Mateusz Nowak, Slawek Nowak, Stavros Papadopoulos, Anastasis Drosou, Dimitrios Tzovaras -- 6. Chariot-integrated Approach to Safety, Privacy, and Security - CHARIOT IPSE / Aydin Ulas, Bora Caglayan, Sofiane Zemouri, George Theofilis, Konstantinos Loupos, Antonis Mygiakis, Andrea Battaglia, Mario Villiani, Christos Skoufis, Stelios Christofi -- 7. Pattern-driven Security, Privacy, Dependability and Interoperability in IoT / Nikolaos Petroulakis, Konstantinos Fysarakis, Henrich C. Pohls, Vivek Kulkarni, George Spanoudakis, Arne Broring, Manos Papoutsakis, Manolis Michalodimitrakis, Sotiris Ioannidis -- 8. Enabling Continuous Privacy Risk Management in IoT Systems / Victor Muntes-Mulero, Jacek Dominiak, Elena Gonzalez, David Sanchez-Charles -- 9. Data

Protection Compliance Requirements for the Internet of Things / Luca Bolognini, Sebastien Ziegler, Pasquale Annicchino, Francesco Capparelli, Alice Audino -- 10. Cybersecurity Certification in IoT Environments / Sara N. Matheu, Antonio F. Skarmeta -- 11. Firmware Software Analysis at Source Code and Binary Levels / Franck Vedrine, Florent Kirchner, Basile Starynkevitch, Andrea Battaglia, Mario Villiani, Konstantinos Loupos -- 12. End-to-End Security for IoT / Paul-Emmanuel Brun, Guillemette Massot -- 13. Blockchain Ledger Solution Affirming Physical, Operational, and Functional Changes in an IoT System / Alexandros Papageorgiou, Konstantinos Loupos, Thomas Krousarlis -- 14. Leveraging Interledger Technologies in IoT Security Risk Management / Dmitrij Lagutin, Yki Kortesniemi, Vasilios A. Siris, Nikos Fotiou, George C. Polyzos, Lei Wu -- Epilogue -- Index -- About the Editor -- Contributing Authors.

Sommario/riassunto

In recent years, the rising complexity of Internet of Things (IoT) systems has increased their potential vulnerabilities and introduced new cybersecurity challenges. In this context, state of the art methods and technologies for security risk assessment have prominent limitations when it comes to large scale, cyber-physical and interconnected IoT systems. Risk assessments for modern IoT systems must be frequent, dynamic and driven by knowledge about both cyber and physical assets. Furthermore, they should be more proactive, more automated, and able to leverage information shared across IoT value chains. This book introduces a set of novel risk assessment techniques and their role in the IoT Security risk management process. Specifically, it presents architectures and platforms for end-to-end security, including their implementation based on the edge/fog computing paradigm. It also highlights machine learning techniques that boost the automation and proactiveness of IoT security risk assessments. Furthermore, blockchain solutions for open and transparent sharing of IoT security information across the supply chain are introduced. Frameworks for privacy awareness, along with technical measures that enable privacy risk assessment and boost GDPR compliance are also presented. Likewise, the book illustrates novel solutions for security certification of IoT systems, along with techniques for IoT security interoperability. In the coming years, IoT security will be a challenging, yet very exciting journey for IoT stakeholders, including security experts, consultants, security research organizations and IoT solution providers. The book provides knowledge and insights about where we stand on this journey. It also attempts to develop a vision for the future and to help readers start their IoT Security efforts on the right foot.